Strategy Research Project

AMERICA'S SOFT UNDERBELLY: ECONOMIC ESPIONAGE

BY

COLONEL KEVIN J. DEGNAN
United States Army

USAWC CLASS OF 2009

U.S. Army War College, Carlisle Barracks, PA 17013-5050

The U.S. Army War College is accredited by the Commission on Higher Education of the Middle State Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

REPORT DOCUMENTATION PAGE

Form Approved
OMB No. 0704-0188

1. REPORT DATE *(DD-MM-YYYY)*	**2. REPORT TYPE**	**3. DATES COVERED** *(From - To)*
10-12-2008	Strategy Research Project	

4. TITLE AND SUBTITLE
America's Soft Underbelly: Economic Espionage

5a. CONTRACT NUMBER

5b. GRANT NUMBER

5c. PROGRAM ELEMENT NUMBER

6. AUTHOR(S)
Colonel Kevin J. Degnan

5d. PROJECT NUMBER

5e. TASK NUMBER

5f. WORK UNIT NUMBER

7. PERFORMING ORGANIZATION NAME(S) AND ADDRESS(ES)
Colonel Stephen Weiler
Department of Command, Leadership, and Management (DCLM)

8. PERFORMING ORGANIZATION REPORT NUMBER

9. SPONSORING / MONITORING AGENCY NAME(S) AND ADDRESS(ES)
U.S. Army War College
122 Forbes Avenue
Carlisle, PA 17013

10. SPONSOR/MONITOR'S ACRONYM(S)

11. SPONSOR/MONITOR'S REPORT NUMBER(S)

12. DISTRIBUTION / AVAILABILITY STATEMENT
Distribution A: Unlimited

13. SUPPLEMENTARY NOTES

14. ABSTRACT
As economic markets change and globalization continues to stretch and stress U.S. corporations, security of corporate and sensitive U.S. technology is increasingly a matter of national security. Threats to sensitive U.S. technologies come not only from our enemies, but from our allies and free market competitors. U.S. industries are a priority for economic espionage and very often a priority target for our adversaries. Foreign companies and governments seek to acquire U.S. technology capabilities in order to technological parity and a competitive advantage with which to enhance their military capabilities. As this national security threat continues to grow, the U.S. government should initiate appropriate counter espionage defense systems to protect U.S. interests and sensitive technologies. Potential solutions include expanding the National Counter Intelligence Executive (NCIX) Office, establishing a standing Interagency Economic Espionage Coordination Group (IEECG) or expanding the Federal Bureau of Investigations Counterintelligence Domain Program (CDP) to counter economic espionage by foreign competitors and adversaries.

15. SUBJECT TERMS
U.S. Technologies, Corporate Security, Military Capability, Globalization

16. SECURITY CLASSIFICATION OF:			**17. LIMITATION OF ABSTRACT**	**18. NUMBER OF PAGES**	**19a. NAME OF RESPONSIBLE PERSON**
a. REPORT	**b. ABSTRACT**	**c. THIS PAGE**			**19b. TELEPHONE NUMBER** *(include area code)*
UNCLASSIFED	UNCLASSIFED	UNCLASSIFED	UNLIMITED	30	

USAWC STRATEGY RESEARCH PROJECT

AMERICA'S SOFT UNDERBELLY: ECONOMIC ESPIONAGE

by

Colonel Kevin J. Degnan
United States Army

Colonel Stephen Weiler
Project Adviser

This SRP is submitted in partial fulfillment of the requirements of the Master of Strategic Studies Degree. The U.S. Army War College is accredited by the Commission on Higher Education of the Middle States Association of Colleges and Schools, 3624 Market Street, Philadelphia, PA 19104, (215) 662-5606. The Commission on Higher Education is an institutional accrediting agency recognized by the U.S. Secretary of Education and the Council for Higher Education Accreditation.

U.S. Army War College
CARLISLE BARRACKS, PENNSYLVANIA 17013

ABSTRACT

AUTHOR: Colonel Kevin J. Degnan

TITLE: America's Soft Underbelly: Economic Espionage

FORMAT: Strategy Research Project

DATE: 10 December 2008 WORD COUNT: 5,738 PAGES: 30

KEY TERMS: U.S. Technologies, Corporate Security, Military Capability, Globalization

CLASSIFICATION: Unclassified

As economic markets fluctuate and globalization continues to stretch and stress U.S. corporations due to increased competition, security of corporate and sensitive U.S. technology is increasingly a matter of national security. Threats to sensitive U.S. technologies come not only from our enemies, but from our allies and free market competitors. U.S. industries are a priority for economic espionage and very often a priority target for our adversaries. Foreign companies and governments seek to acquire U.S. technology capabilities in order to achieve technological parity and a competitive advantage with which to enhance their military capabilities.[1] As this national security threat continues to grow, the U.S. government should initiate appropriate counter espionage defense systems to protect U.S. interests and sensitive technologies. Potential solutions include expanding the National Counter Intelligence Executive (NCIX) Office, establishing a standing Interagency Economic Espionage Coordination Group (IEECG) or expanding the Federal Bureau of Investigation's Counterintelligence Domain Program (CDP) countering economic espionage by foreign competitors and adversaries.

AMERICA'S SOFT UNDERBELLY: ECONOMIC ESPIONAGE

One of the United States' greatest societal strengths is its openness. This strength, however, is developing into one of our greatest weaknesses as globalization and interconnected economies transform state-to-state relationships. Our society's natural state of openness creates strategic and economic vulnerabilities whereby foreign nations, both Allies and adversaries, can target our research and development (R&D) centers, private corporations, universities or other American institutions for cutting edge and developing technology, and intellectual property for theft. "The openness of American government and society makes us vulnerable … all our institutions are at risk."[2] The U.S's friends and foes are targeting its institutions and private entities to advance their national interests and promote their market positions, while undermining U.S. policy, eroding our economic power, weakening our alliances and eliminating our technological advantages. Historically, this threat is not totally new as demonstrated in the case of Ethel and Julius Rosenberg sharing atomic secrets with the Soviet Union during World War II. In today's post Cold War world, the effects of economic espionage on U.S. national security and economic power are potentially catastrophic. The U.S. must put systems in place to deter and defeat economic espionage while simultaneously protecting sensitive U.S. technologies in a globalized world.

Economic espionage threats from U.S. Allies and adversaries alike are growing in intensity, sophistication and frequency. Robert Mueller, Director of the FBI, has assessed this threat to be so grave that he has designated espionage as the FBI's number two priority second only to terrorism.[3] The two oceans that have secured our

flanks and provided geographic strategic security in previous centuries are no longer enough to protect the U.S. America's soft underbelly, its openness, makes its economic and military power increasingly vulnerable to erosion in a globalized world as other nations develop their economies and military capabilities. This paper is a clarion call for strong action against economic espionage. Furthermore, this paper draws attention to economic and military espionage, highlights specific case examples including tactics, and concludes with a recommendation: the U.S. should urgently prioritize the counter-economic espionage function in our government to secure and enhance our national security and preserve our economic power.

"Economic espionage costs U.S businesses anywhere from $45 billion to as much as $250 billion annually."[4] During the decade of the 1980's espionage is estimated to have cost U.S. business as much as $1.2 trillion dollars.[5] While these figures represent a staggering financial drain for American corporations, this represents a loss of employment for American workers and tax revenue for state and the federal government. Our competitors and adversaries are undermining our economic power through numerous espionage methods as they erode U.S. technological advantage in both economic and national military power. Private industry, which is the foundation for our economic power and military superiority, is being undermined through the theft of intellectual capital, trade secrets, and classified information. The U.S. is becoming increasingly dependent on the very informational and communication technologies which function to increase our vulnerabilities to economic espionage and cyber theft. No single government agency in the U.S. can clearly estimate the overall number of espionage acts perpetrated against economic or military sectors. The FBI estimates that

only 17% of companies victimized by cyber espionage report it to law enforcement agencies due to fear of loss of consumer confidence and depreciation of stock value.[6] This lack of reporting economic espionage events exacerbates the problem.

In 1996, Congress passed and President Clinton signed into law the Economic Espionage Act (EEA). The law was passed to counter increasing domestic and international espionage threats to the U.S. and American corporations with bipartisan support. Acknowledging concern for this growing threat, the House of Representatives passed the EEA with 399 members in support, 3 members against and 31 members abstaining. The Senate passed the bill unanimously.[7] Since the end of the Cold War, the targeting of U.S. corporations for espionage and their trade secrets has dramatically increased.[8] Espionage is defined as an organized effort by one country's government to acquire vital national security secrets of another country.[9] The intent of the EEA law is to provide a "federal remedy targeting the theft of trade secrets" to help protect economic and military sectors of the U.S. economy.[10] Trade secrets are one of the three proprietary economic information categories. The other two are patented inventions and copyrighted material.[11] Theft of trade secrets is becoming the dominant threat against corporate America.[12] The law punishes those who willfully,

> Misappropriate, or attempt or conspire to misappropriate, trade secrets with the intent or knowledge that their offense will benefit a foreign government, foreign instrumentality, or foreign agent.[13]

This law is intended to protect U.S. economic power from being illegally eroded by foreign governments, foreign agents or foreign corporations. The law is designed to protect our national security interests.

Economic espionage is a complex and diverse field of study with many vantage points that could be examined and studied. Economic espionage is exploiting and

undermining both American businesses and national security interests. This paper focuses on a single state actor conducting economic espionage for economic or corporate benefit and a single state actor conducting espionage targeting U.S. corporations or institutions that support the Department of Defense and national security interests. Espionage which targets economic or corporate advantage is defined as "*Business Espionage*" (BE) while that which targets military or sensitive technology is defined as "*Military Espionage*" (ME).

Threats to U.S. Economic and Military Power – Is there a Strategy?

In 1999, the top six countries engaged in economic espionage against U.S. business interests were China, Japan, England, France, Canada and Mexico.[14] The two largest threats to U.S. business espionage and military espionage (ME) come from Japan and China respectively. This paper considers the significance and depth of the problem and makes a case for greater counter-espionage action by the U.S. government.

Sun Tzu provides some insight into the strategic thinking employed by our competitors and adversaries in securing BE and ME knowledge and technology. Sun Tzu understood the economic factors in war and advised securing 'foreknowledge' from one's rivals (enemies) through the deployment of agents. He explains five types of agents that work in a system to the benefit of the state. The types are: the Native, Inside, Doubled, Expendable and Living.[15]

Sun Tzu explains that a Native Agent is a person from the targeted country we employ. This could be an American lobbyist hired by the Chinese government to secure favorable trade policy. An Inside Agent is a rival official who covets wealth, is deceitful

and will take advantage of troubled times for self promotion. An American dissatisfied with his pay for hi-tech work could be targeted as an Inside Agent. Double Agents are enemy spies that an adversary exploits and employs by having them double-cross their country. Expendable Agents are used to spread false information or to unwittingly deceive the enemy of true intentions. A simple example of this technique is to leak false information to your adversaries to mask one's true intent. Living Agents are entrusted to gain access to the enemy's detailed plans and operations and to report the information back.[16] This type agent must have excellent access to sensitive adversary information and secure trust. Sun Tzu advises, "Those skilled in war subdue the enemy's army without battle. They capture his cities without assaulting them and overthrow his state without protracted operations."[17] Considering the use of agents by our adversaries in economic espionage, it is feasible for grave damage to be done to U.S. national security.

Sun Tzu's counsel helps to clarify how an adversary might employ agents to exploit and undermine U.S. economic power. The point is not to argue that Sun Tzu's strategy is being employed by U.S. competitors or adversaries, but to suggest that some elements of Sun Tzu's strategy of securing "foreknowledge" through the use of spies is being employed against the U.S. In the case of Japan and China, the examples that follow demonstrate espionage activities to secure foreknowledge and gain BE and ME advantage. As Sun Tzu advises in The Art of War, they are doing so through an elaborate network of spies and well placed agents to gain intelligence and advantage. The illustrations below highlight but a few cases.

Japanese Threat to US Economic Power

In the 1980's, Japan set up a comprehensive network of laboratories around university towns to capture new technologies. They gained foreknowledge by identifying and securing over 40,000 patents from work being done by U.S. universities. U.S. experts from the National Research Council concluded that these efforts enabled them to take command of the television and semiconductor market which essentially drove U.S. competitors out of business.[18]

The Japanese espionage network against the U.S. is comprehensive and robust. This spy network entails Living and Inside Agents as characterized by Sun Tzu. In 1988 alone, Japan sent 52,224 researchers to the U.S whereas the U.S. sent less than 4,500 to Japan.[19] The Japanese systematically positioned intelligence and subject matter expert personnel to take advantage of U.S. research and product development. A Japanese intelligence firm president confirmed this tactic:

> When a Japanese company wants to expand into an international market, it opens a small outpost there to learn as much as it can about that market and about competitors it will be facing … they look to acquire intelligence as a pre-investment to their marketing plan.[20]

In 2001, a grand jury indictment charged two Japanese 'Living Agents' with two counts of violating the EEA for the theft of research into the cause and potential cure of Alzheimer's disease.[21] They were attempting to steal the deoxyribonucleic acid (DNA) and the cell line reagents from the Cleveland Clinic Foundation (CCF) while also corrupting the remaining DNA and cell lines. Mr. Takashi Okamoto, an employee of the Lerner Research Institute of the CCF, was trying to bring the stolen material home to Japan. Hired by Institute of Physical and Chemical Research (Riken) in Japan (which received 94% of its funding from the Japanese Ministry of Science and Technology), Mr.

Okamoto and his accomplice were attempting to steal U.S. research and subsequent knowledge and artifact.[22]

More recently, on July 1st, 2008 the U.S. Supreme Court upheld a $4.3 million ruling against Toyota Motor Corporation (TMC) for patent infringement dating back to 2005 for using patented designs equivalent to those of Paice LLC, of Bonita Springs, Florida.[23] The court found in favor of Paice LLC that TMC infringed upon patent no. 7,392,871 entitled Hybrid Vehicles currently being employed in the Highlander SUV and the Lexus RX400 SUV.[24] In this court action, Paice LLC sought to affirm Toyota's willful patent infringement, to permanently forbid Toyota from using patent 7,392,871 on future vehicles and sought other relief as the court deemed appropriate.[25] In essence, "Toyota made use of a microprocessor which accepts torque information from the electric motor and internal combustion engine" for the Hybrid Synergy Drive (HSD) system which is also used on the Toyota Prius, their flagship hybrid vehicle.[26] In addition to the one-time patent infringement violation fee of $4.3 million, Toyota has been directed to pay Paice LLC a fee of $25 dollars for every Prius, Highlander Hybrid and Lexus RX400h sold.[27] The final Supreme Court ruling did not preclude the Japanese car company from continuing production and sales of their hybrid vehicles with stolen U.S. technology from Paice LLC. This particular patent infringement may seem relatively insignificant, but in the globalized marketplace where competition is fierce and U.S. automobile companies are on the verge of bankruptcy, any advantage secured through BE affords a significant competitive advantage. In this case, Toyota's advantage is combined with an ailing U.S. auto industry, record high gas prices, and advanced hybrid technology providing a niche

capability that significantly enhances fuel mileage, which is one of the top three consumer decision criteria in purchasing a new car.[28]

In this BE patent infringement case, U.S. courts have permitted Toyota to continue manufacturing and selling the Paice LLC designed hybrid technology even though their patent had been infringed upon. Paice LLC will receive a small stipend for each Toyota sold with their microprocessor HSD system technology. The court's decision, however, appears to be a very small punishment for BE patent theft. If foreign corporations are not deterred from stealing U.S. technology through stiff penalties and significant actions, then the courts are de facto inviting more espionage against American interests.

Clearly, globalization is providing unprecedented access to U.S. markets and enabling foreign corporations to build constituencies in the U.S. Once foreign companies are entrenched in U.S. society as Toyota is, they wield tremendous influence in American society due to their economic power in job and wealth creation. As foreign influence expands through globalization in the U.S. economy, our U.S. court system should give priority consideration to American corporations disadvantaged by economic espionage in upholding the law.

Threats to U.S. Military Superiority – Espionage by China

In testimony to a House Subcommittee on espionage law enforcement, Mr. Larry Wortzel, who chairs the Unites States-China Economic and Security Review Commission, assessed China's espionage activities as the "single greatest threat to U.S. technology."[29] He added that the People's Republic of China (PRC) espionage activities benefits their development of new technology without the time and money

necessary to conduct research.[30] Mr. Wortzel details China's centralized approach to their espionage practices through their "863 Program" also known as their "Torch Program."[31] In the Torch espionage program, China coordinates espionage activities targeting biotechnology, space technology, information technology, laser technology, automation technology, energy technology and advanced materials to include dual-use components that can be used to benefit their military as well.[32]

The People's Republic of China (PRC) has been involved in orchestrating sophisticated espionage programs designed to steal sensitive U.S. military technology. In many cases the PRC is recruiting naturalized Chinese U.S. citizens well placed in U.S. military and/or industry to conduct ME. In one high profile case in 2008, the FBI indicted and arrested a Chinese naturalized U.S. citizen on eight counts of economic espionage, one count of conspiracy to commit espionage and for acting as an unregistered agent of the PRC.[33] Mr. Dongfan Chung, a retired Boeing engineer, is alleged to have stolen military trade secrets involving the Space Shuttle, the C-17 military transport aircraft and the Delta IV rocket.[34] According to the indictment, Chung received tasking letters from the PRC. Between 1985 and 2003 he made numerous trips to China to lecture on technology and during these trips he met with officials and agents of the PRC.[35] Consistent with Sun Tzu's recommendation to conduct espionage and gain foreknowledge, the PRC targets Chinese naturalized American citizens to be their 'Living Agents' using nationalism and financial reward to entice them into spying for the "motherland." As the FBI details, people of the same cultural, ethnic and national backgrounds are targeted to help create their spy network for ME purposes by the PRC.[36]

In another high profile case of Chinese espionage, a federal grand jury in California found Chi Mak, "guilty of conspiring to violate export control laws and acting as a foreign agent without registering" in May 2007.[37] This case involved the theft of sensitive U.S. radar technology and quiet-drive naval technology. Most concerning and demonstrating the new vulnerabilities in a globalized world is the fact that Chi Mak was not a U.S. government employee, but was employed by a subsidiary of the L3 Corporation. As Dr. Joel Brenner from the Office of National Counterintelligence Executive (ONCIX) and Mission Manager for Counterintelligence points out, government contractors are changing the nature of the insider threat and vulnerabilities now extend to the private sector, as well as the public sector.[38] Dr. Brenner warns of the nexus between the private sector and academia as being easy targets for foreign intelligence efforts as is demonstrated in the Chi Mak case. Private industry faces risks that extend well beyond classified work in private industry such that the boundary between public and private sectors is all but vanishing.[39]

Between the periods of March 2007 through March 2008, twelve cases of Chinese espionage were disclosed in open source reporting. These cases involve the PRC targeting sensitive U.S. military technologies including controlled power amplifiers used in digital radios, night-vision technology including goggles, cruise missile technology, and source code for simulation software used for training pilots.[40] In one significant case, U.S. export controls were grossly violated by ITT Corporation in which they exported night-vision data to China, Singapore and Great Britain.[41] For failing to follow U.S. export control laws, ITT Corporation has been fined $100 million dollars.

Several similar cases involved the use of naturalized Chinese American citizens as in the Chi Mak and Dongfan Chung cases.

China's aggressive spying, technology theft, illegal acquisition of restricted military technology and computer attacks is posing an increasingly serious threat to U.S. national security and military power.[42] After attending the United States-China Economic and Security Review Commission Hearing Congressman Randy Forbes assesses that "China has become the No. 1 espionage threat to the United States" and added that this increasing threat will eventually put American soldiers at risk.[43] Underpinning the ME and BE Chinese threat is the U.S.-Chinese trade imbalance of five to one or $1.68 billion; Chinese defense modernization and growth from industrial espionage and dual-use commercial transfers of technology; and the $1 trillion of U.S. foreign currency reserves of U.S. government or corporate bonds.[44] The trade imbalance and subsequent loss of jobs is a most sensitive issue with American workers and many politicians. Since 1998 America has lost 3.4 million manufacturing jobs, with an estimated 1.3 million of them going to China as a direct result of out-sourcing and business relocation.[45]

Threat from Globalization Embeds in U.S. Economy

Globalization is "the international integration of markets, goods, services and capital."[46] The major issues concerning globalization for the U.S. are centered on the potential loss of economic power and its technological superiority being "leveled" as emerging countries such as India, China, Israel and Taiwan stimulate innovation and technology within their economies.[47] The key U. S. challenge is to maintain its

economic power and technical military superiority in a globalized world while safeguarding national security and mitigating the risks.

"Globalization, while generating major gains for the U.S. economy, has given foreigners unprecedented access to U.S. firms and sensitive technologies."[48] Trade secrets and intellectual property are more at risk today than at any other time in U.S. history.[49] Foreign governments and entities are using a variety of techniques to gain access to U.S. government installations and corporate entities. Of the 30 million visitors to the U.S. in 2005 alone, nearly 5 million entered on business visas. Many of these visitors gained access to U.S. technology through business interests that appear harmless. However, this challenges the U.S. government and industry to protect sensitive technologies that have dual-use trade secrets for both commercial and military application.[50] The U.S. counterintelligence community assesses that "foreign governments are major beneficiaries of private-sector technology flow" and that foreign nationals and first generation immigrant Americans working in scientific and technological fields are being targeted for disclosure through financial enticement, nationalism to their home country or scientific acclaim.[51] Clearly, this has been proven true in the case of China as detailed in several cases outlined above.

The Office of National Counterintelligence Executive breaks down the types of directed foreign collectors in the U.S. targeting defense technology in 2005 as follows; Government related 29%, Government 23%, Commercial 24%, Individual 10% and unknown 14%. This is a best estimate considering it is very difficult to differentiate between public (government) and private (corporate) in the theft of technology due to

the increasing complexity association with public-private financing (as is often the case with China, Russia and other Asian and European countries.) [52]

Moreover many other concerns are setting the conditions for continued U.S. vulnerability to technological theft and economic erosion. Approximately 30% of science and engineering students at U.S. universities are foreign born.[53] More than 40% of PhDs awarded in science and engineering departments were to foreign citizens while 55% of physics and math PhDs were awarded to foreign citizens.[54] U.S firms are hiring foreign employees out of necessity with a dwindling number of Americans with technical degrees to choose from. Our university system is growing the world's technological experts but our country is not fully benefitting from this investment in human resources. Foreign employees make U.S. corporations more vulnerable to espionage activities as their loyalty and commitment to U.S. ideals are not inculcated from birth as citizens. This has been demonstrated as in many of the Chinese espionage cases. Foreign governments and competitors actively recruit their countrymen and those of the same national background to engage in economic espionage.[55]

Challenges to Countering Espionage

Pitfalls associated with the EEA make many corporations hesitant to take legal action in response to foreign theft of corporate trade secrets for a several reasons. Corporations may choose to not elevate the issue for fear of bad publicity, more public disclosure of the trade secret, negative effects on stock value or somehow managing to reach a private settlement with the perpetrator.[56] Perhaps the biggest reason a company may hesitate to take action is that once the Department of Justice (DOJ) decides to take the case, the company loses all control over the matter and whether or

not vital information will be made public either during discovery or trial proceedings.[57] The DOJ should be more sensitive to these legitimate concerns in order to help bring these cases to the surface in countering the overall BE and ME threat.

In 2007 the Honorable John D. Negroponte, Director of National Intelligence (DNI), addressed the issue of globalization, its impact on U.S. security, and the growing economic espionage threat to the U.S. In the DNI's Annual Threat Assessment on US National Security Challenges document and in his testimony to the Senate Select Committee on Intelligence, he said:

> Globalization also exposes the U.S. to mounting counterintelligence challenges. Our comparative advantage in some areas of technical intelligence, where we have been dominant in the past, is being eroded … A significant number of states also conduct economic espionage … The challenge we face is not catching up to globalization or getting ahead of it – it is recognizing the degree to which our national security is inextricably woven into the fabric of globalization.[58]

Countering Espionage & Protecting U.S. Economic and Military Power

Since the attacks of September 11, 2001 the U.S. government has been working to effectively put in place a counterintelligence system that is capable of identifying and countering threats on a broad range of issues. The Counterintelligence Act of 2002 and subsequent Intelligence Reform and Terrorism Prevention Act (IRTPA) of 2004 are part of the protection system.[59] The IRTPA charged the office of The National Counterintelligence Executive (NCIX) with the responsibility to protect vital national assets and to develop a strategy for integrating counterintelligence activities "to better protect America's secrets and vital assets while providing incisive intelligence to national security decision makers."[60] The strategy directs the nation's counterintelligence elements to operate as a unified, joint "coherent community" in

support of the priorities as directed by NCIX.[61] The first priority established in the strategy is "Secure the nation against foreign espionage and electronic penetration.[62]

The FBI's Role. The Federal Bureau of Investigation (FBI) is responsible for combating economic espionage. To counter Chinese BE and ME, the FBI has increased the number of agents from 150 in 2001 to 350 in 2007.[63] The FBI has assessed significant counterintelligence weaknesses making U.S. companies "easy prey for foreign intelligence services, foreign organizations and foreign competitors."[64] Toward this end, the FBI has initiated an outreach program where the FBI conducts seminars for U.S. corporations to highlight counterintelligence vulnerabilities and educate corporation Chief Executive Officers on the growing espionage threat of the "Insider Danger." The "Insider Danger" threat refers to a tiny minority of foreign born employees hired by U.S. companies who cause devastating damage by stealing corporate secrets for a foreign government or a commercial entity.[65] This paper illuminated a few of the Chinese cases of espionage. Furthermore, Wired magazine expounds upon this type of threat warning to keep a close eye on H1-B visa employee hires. Wired highlights two foreign hire employee espionage practices as follows:[66]

> Case One is a foreign-born engineer who has been educated in the U.S. Over a 10 – 15 year period, she rises to mid-level management. Then she returns to her home country and gets paid by her government to compete with U.S. businesses.
>
> Or
>
> Case Two is a series of university students' or professors' from overseas take jobs in university research labs and then get involved in related military projects. Individually, they learn only bits and pieces. But collectively, they pass the information back to their home country and it paints a telling picture of our country's defense initiatives.

Because of the Chinese insider threat among others, FBI Director Robert Mueller has assessed this threat as "substantial and directed the FBI to increase counterintelligence efforts" as we have seen a dramatic increase in the number of agents.[67]

Countering Economic Espionage - A Good Start

The statement below by Timothy D. Bereznay, Assistant Director for the FBI Counterintelligence Division, highlights the gravity of the situation in addressing the need for the Export Enforcement Initiative (EEI) announced in October 2007 to confront the growing threat of foreign acquisition of restricted U.S. technology.

> The theft of intellectual property and technology by foreign parties or governments directly threatens both the national and economic security of the U.S. in which the development and manufacturing of U.S. products results in weakened economic capability and diminished political stature for this country.[68]

In this plan, the Departments of Justice, Homeland Security, Commerce, U.S. Immigrations and Customs Enforcement, the Defense Criminal Investigative Service and the FBI have formed counter-proliferation Task Forces (TF) in U.S. Attorney's offices around the country. These multi-agency TFs focus on prevention, cooperation and coordination to counter illegal foreign acquisition of U.S. technology.[69] Under its Counterespionage section, the Justice Department has appointed its first National Export Control Coordinator to implement, coordinate and train staff to implement this initiative. As part of this effort, these TF's educate industry regarding the threat and share information to prevent foreign efforts to secure U.S. technology.[70]

The FBI has also initiated the Counterintelligence Domain Program (CDP) to "protect sensitive information, technologies and U.S. competitiveness in an age of globalization."[71] The CDP consists of two components, the Business Alliance (BA) and

the Academic Alliance (AA) outreach efforts. The purpose of the BA is to build relationships with U.S. defense contractors to educate them on foreign intelligence services and foreign competitive threats to help them safeguard sensitive technologies and information.[72] Outreach to AA serves a similar purpose briefing university presidents and leadership on potential threats to their institutions through the research and development realm, which subsequently has a negative effect on U.S. national security.[73]

The Export Enforcement Initiative (EEI) and the Counterintelligence Domain Program (CDP) are two good initiatives to assist in countering the ME and BE threat to U.S. national security. Considering a 43% increase in the number of suspicious foreign contacts targeting U.S. defense firms from a record 108 countries since 2006, clearly aggressive action is needed.[74] Multiple programs operated by varying agencies run the risk of creating seams, duplication of effort or worse, failing to gather threats missed through a lack of coordination. Similar to other government initiatives to fuse, share and coordinate information to counter threats, it may be time to empower a single organization or designate a standing Joint Interagency Coordination Group to counter the BE and ME threats to our nation.

Way Ahead: Empower an Organization or an Interagency Coordination Group

A single government organization fully integrated with counterespionage resources is needed to effectively counter the growing BE and ME threat. While some government structure has been put in place to conduct counterespionage activities over the last several years, it is bifurcated in the Department of Defense, NCIX under the Department of National Intelligence and the FBI under the Department of Justice. Three

options are identified for better aligning U.S. government counterespionage resources coherently with the assets and authority in a single organization to perform the mission. All three options are feasible, acceptable and suitable in deterring, identifying and defeating economic espionage to counter the growing BE and ME threats to U.S. military and economic power. Most importantly, these options will help strengthen counterintelligence programs and activities of the U.S. government as Congress directed in the National Counterintelligence Enhancement Act of 2002.[75] Three options are broadly presented with brief descriptions, strengths and weaknesses, and are followed by a final recommendation for U.S. government action.

Option One. Grow the Mission of the National Counter Intelligence Executive. Under this option, the President issues a Presidential Directive designating the National Counter Intelligence Executive (NCIX) as the lead government organization to deter and defeat economic espionage directed against U.S. national security interests. The NCIX would be assigned the additional mission of protecting America's economic security along with its other five mission essential tasks.[76] This benefits the federal government by building upon the NCIX organization established in the National Counterintelligence Enhancement Act of 2002 and subsequent IRTPA in 2004 to counter terrorism. These same resources would serve to counter economic espionage with only a modest augmentation of interagency resources. Already charged with "securing the nation against foreign espionage and electronic penetration," this would enhance the NCIX with FBI and interagency augmentation to identify threats, enforce the law and prosecute espionage.[77] The strengths of this option are it is a cost effective approach utilizing counterintelligence resources already in place that is consistent with the other

missions performed by NCIX and builds upon laws put in place in 2002 and 2004. The weaknesses of this option are it will require augmentation of personnel from the interagency, an increase in NCIX personnel and budget authority and prosecution authority for espionage resides in the FBI. Of the three options outlined in this paper, this is assessed as being moderately expensive.

Option Two. Establish a Standing Interagency Economic Espionage Coordination Group (IEECG). The President issues a Presidential Directive establishing a permanent IEECG stand-alone organization that reports to the Director of the FBI to organize the U.S. government to counter, deter and defeat economic espionage directed against U.S. national security interests. The IEECG would be chartered to coordinate threat information and awareness to both commercial and public entities at the federal, state and local levels. It would consist of representatives of all core governmental agencies involved in counterintelligence activities which includes the FBI Counterintelligence Division, the DNI's National Counterintelligence Executive (NCIX), DoD Services counterintelligence elements, academia and business community organizations to advise, warn and coordinate economic espionage threats and information. The IEECG would be modeled after the Interagency Threat Assessment and Coordination Group (ITACG) established by President Bush as one of the recommendations from the 9/11 Commission Act of 2007 to improve the sharing of information at the federal, state, local and private sector to counter terrorism.[78]

The major strength of this option is that it provides a singularly focused organization to deter and defeat espionage while incorporating an interagency approach to coordinate activities. The weaknesses of this option include standing up a new

organization with personnel, budget and authority that will likely take time to be effective. This is the most expensive option. In the long run, however, benefits will outweigh costs as espionage is deterred and defeated through better coordination and information exchange between governmental agencies, academia and corporate industry. This option would establish a direct reporting chain to the Director of the FBI to counter economic espionage activities. Furthermore, education and training of foreign threats and activities would be emphasized in outreach programs to government agencies, academia and corporate industry.

Option three. Expand the FBI's Counterintelligence Domain Program (CDP) and Designate as the Office of Primary Responsibility for the Federal Government. Under this option, the President issues a Presidential Directive designating the FBI's Counterintelligence Domain Program as the lead government organization to counter, deter and defeat economic espionage directed against U.S. national security interests. This benefits the federal government by leveraging the CDP's current mission, enhancing it with interagency resources to coordinate counter espionage activities and saves money by not standing up a new organization that does not exist today. The CDP would continue to counter espionage activities through conference participation, visiting industry as an outreach initiative and further developing its work with state and local law enforcement and imbedding intelligence community personnel within the CDP to counter economic espionage.[79] The primary advantage of this option is the CDP would expand to be an interagency organization leveraging its organic legal authority and jurisdiction to enforce the Economic Espionage Act of 1996 prosecuting foreign agents or foreign instrumentalities found to be in violation of the law. Interagency personnel and

resources would help foster close coordination and bring all information elements together in a single organization to counter the threat. The weaknesses of this option are similar to option one. It will require augmentation of personnel from the interagency and an increase in CDP personnel and budget authority. Of the three options outlined in this paper, this is assessed as being the least expensive and most effective.

Recommendation

When weighing cost, structural alignment, ability to have an immediate impact and organizational authorities to enforce the law, Option Three is the best course of action to counter BE and ME. Expanding the FBI's Counterintelligence Domain Program and designating it as the office primarily responsible for federal counter economic espionage serves to leverage intrinsic authorities while minimizing costs and facilitating rapid response. Mission analysis should be initiated to determine what resources are needed from interagency organizations to successfully consolidate the BE and ME mission to counter, deter and defeat economic espionage against the U.S. Lastly, the CDP should be renamed the National Counter Economic Espionage Office to align the office name with the mission and serve as a deterrent to this growing threat.

Conclusion

This paper makes a clarion call for strong action to be taken to counter the growing threat of economic espionage. As highlighted in specific case examples, U.S. national security is under assault through acts of espionage by our Allies and adversaries alike in both the economic and military realms of American society. Until we get more serious about deterring and defeating espionage through enhanced organizational structure and comprehensive countermeasures, we remain a nation at

risk marginally postured to prevent our technology advantages in industry and military capabilities from being slowly eroded.

Endnotes

[1] Mr. Peter Schweizer, "The Growth of Economic Espionage: America is target Number One," Foreign Affairs, (January/February 1996): Lexis/Nexis (Accessed August 12, 2008).

[2] Norman B. Imler, "Espionage in an Age of Change: Optimizing Strategic Intelligence Service for the Future," in *Intelligence and the National Security Strategist: Enduring Issues and Challenges*, ed. Roger Z. George and Robert D. Kline (Washington DC: National Defense University Press, 2004), 226.

[3] The Federal Bureau of Investigations, http://www.fbi.gov/hq/ci/economic.htm (accessed October 28, 2008).

[4] Steven Fink, Sticky Fingers (Chicago, IL: Dearborn Trade Books, 2002), 7.

[5] Ibid.

[6] Hedieh Nasheri, Economic Espionage and Industrial Spying (New York: Cambridge University Press, 2005), 97 and113.

[7] U.S. Congress, "Final Vote Results for Roll Call 416," September 17, 1996 http://clerk.house.gov/evs/1996/roll416.xml (accessed November 4, 2008).

U.S. Library of Congress, "H.R. 3723," September 18, 1996 (http://thomas.loc.gov/cgi-bin/bdquery/z?d104:HR03723:@@@S.

[8] David J. Loundy, Computer Crime, Information Warfare and Economic Espionage (Durham, NC: Carolina Academic Press), 558.

[9] Ibid, 545.

[10] Ibid, 545.

[11] Ibid, 544- 545.

[12] Ibid, 558 – 559.

[13] Ibid, 559.

[14] Fink, Sticky Fingers, 51.

[15] Samuel B. Griffith, Sun Tzu *The Art of War* (New York: Oxford University Press, 1963), 40 and 145.

[16] Ibid, 145 – 147.

[17] Ibid, 79.

[18] John J. Fialka, *War By Other Means* (New York: Norton & Company, 1997), 10 – 11.

[19] Ibid.

[20] A. Coskun Samli and Laurence Jacobs, "Counteracting Global Industrial Espionage: A Damage Control Strategy," *Business and Society Review* 108:1 (Month/year): 103.

[21] Nasheri, Economic Espionage and Industrial Spying, 142.

[22] Ibid, 142 – 144.

[23] Paice LLC, Plaintiff vs. Toyota Motor Corporation, a Japanese Corporation, Toyota Motor North America, Inc, Defendants, Case No.: 2:08-cv-261, Jury Trial Demanded, U.S. District Court for the Eastern District of Texas Marshall Division, July 1, 2008; pp 1-5.

[24] Ibid, 2-3.

[25] Ibid, 4.

[26] Jeremy Korzeniewski, "Toyota Loses Hybrid Patent Appeal Case," May 12th, 2008, linked from http://www.autobloggreen.com/tag/paice+llc/ (accessed September 22, 2008).

[27] Damon Lavrinc, "Toyota Losses Patent Appeal in Prius," May 12th, 2008, linked from http://www.autoblog.com/2008/05/12/toyota-lose-patent-appeal-for-prius/ (accessed September 23, 2008).

[28] Buying Advice.Com, "After Price, Reliability is the Number One Factor for Buyers," October 2, 2008, http://www.buyingadvice.com/top-factors-survey.html (accessed October 2, 2008).

[29] Larry M. Wortzel, Before the House, Subcommittee on Crime, Terrorism and Homeland Security of the House Committee on the Judiciary Hearing on Enforcement of Federal Espionage Laws (January 29, 2008), 2.

[30] Ibid.

[31] Ibid, 3.

[32] Ibid, 3 – 4.

[33] Department of Justice, "Former Boeing Engineer Charged with Economic Espionage in Theft of Space Shuttle Secrets for China," February 11, 2008, http://www.usdoj.gov/opa/pr/2008/February/08_nsd_106.html (accessed September 26, 2008).

[34] Ibid.

[35] Ibid.

[36] Federal Bureau of Investigations, Investigative Programs Counterintelligence Division, "Focus on Economic Espionage," http://www.fbi.gov/hq/ci/economic.htm (accessed November 4, 2008).

[37] Joel F. Brenner, "DNI's Private Sector Symposium on Insider Threats," Welcoming Remarks, Carnegie Endowment for International Peace, Washington, DC, 30 May 2007.

[38] Ibid.

[39] Ibid.

[40] "Recent Espionage Cases Involving China," Washington Post, April 3, 2008, A10.

[41] Ibid.

[42] "Beijing espionage poses 'No. 1' threat," January 30, 2008, linked from *The Washington Times Home Page* at http://www.washingtontimes.com/news/2008/jan/30/beijing-espionage32poses-no-1-threat/ (accessed October 14, 2008).

[43] Ibid.

[44] 2007 Report to Congress of the U.S.-China Economic and security review Commission, 110th Cong., 1st sess., November 2007, 1 – 10.

[45] UCLA Asian American Study Center, "U.S./China Media Brief," http://www.aasc.ucla.edu/uschina/trade_tradeimbalance.shtml (accessed November 5, 2008).

[46] James A. Lewis, CSIS Report: Globalization and National Security (Washington DC: The CSIS Press, December 2004), 1.

[47] Ibid, 5.

[48] U.S. Office of the National Counterintelligence Executive, Annual Report to Congress on Foreign Economic Collection and Industrial Espionage – 2005 (Washington DC: Office of the National Counterintelligence Executive, August 2006), iii.

[49] Ibid, 2.

[50] Ibid, 2.

[51] Ibid, 2-4.

[52] Ibid, 3 – 5.

[53] Ibid, 5.

[54] Ibid, 5.

[55] The Federal Bureau of Investigations, http://www.fbi.gov/hq/ci/economic.htm (accessed November 5, 2008).

[56] Andrew Grosso, “The Economic Espionage Act: Touring the Minefields,” *Communications of the ACM* no. 43.8 (August 2000): 15. (accessed September 22, 2008).

[57] Ibid.

[58] John D. Negroponte, “Annual Threat Assessment and U.S. National Security Challenges,” Statement for the Record to the Senate Select Committee on Intelligence (January 11, 2007).

[59] J. M. McConnell, The National Counterintelligence Strategy of the Unites States of America (Washington DC: Director of National Intelligence), iv.

[60] Ibid, 5.

[61] Ibid, 1.

[62] Ibid, 1.

[63] David J. Lynch, “FBI goes on offensive against China’s tech spies,” *USA Today*, July 25, 2007.

[64] Ibid.

[65] Ibid.

[66] Luke O’Brien, “FBI warns of Spies Disguised as Foreign Engineers,” July 9, 2007, linked from Wired Blog Network at http://blog.wired.com/27bstroke6/2007/07/fbi-warns-of-sp.html (accessed 11 October 2008).

[67] Bill Gertz, “FBI calls Chinese espionage substantial,” *The Washington Times*, July 27, 2007.

[68] U. S. Department of Justice, Justice Department and Partner Agencies Launch National-Proliferation Initiative (Washington DC: U.S. Department of Justice, October 11, 2007), 2.

[69] Ibid.

[70] Ibid, 2-3.

[71] The Federal Bureau of Investigations, http://www.fbi.gov/hq/ci/domain.htm (accessed October 20, 2008).

[72] Ibid.

[73] Ibid.

[74] U. S. Department of Justice, Justice Department and Partner Agencies Launch National-Proliferation Initiative, 1.

[75] J.M. McConnell, Director of National Intelligence, The National Counterintelligence Strategy of the United States of America 2007 (Washington DC: Director of National Intelligence), iii.

[76] The Office of the National Counterintelligence Executive lists five mission essential tasks they are responsible for. These tasks as: (1) Exploit and defeat adversarial terrorists activities directed against U.S. interests (2) Protect the integrity of the U.S. intelligence system (3) Provide incisive, actionable intelligence to decision makers at all levels (4) Protect vital national assets from adversarial intelligence activities and (5) Neutralize and exploit adversarial intelligence targeting the armed forces. Protecting U.S. economic security would become its sixth core task. NCIX, http://www.ncix.gov/about/mission.html (accessed October 30, 2008).

[77] J.M. McConnell, Director of National Intelligence, The National Counterintelligence Strategy of the United States of America 2007 (Washington DC: Director of National Intelligence), 1.

[78] Interagency Threat Assessment and Coordination Group, http://www.ise.gov/pages/partner-itacg.html (accessed October 21, 2008).

[79] Dr. Amelia Augustus, Director *Women's Economic Round Table* of the Knight-Bagehot Program, Economic Espionage, The Journalism School, Columbia University, http://www.journalism.columbia.edu/cs (accessed October 28, 2008)